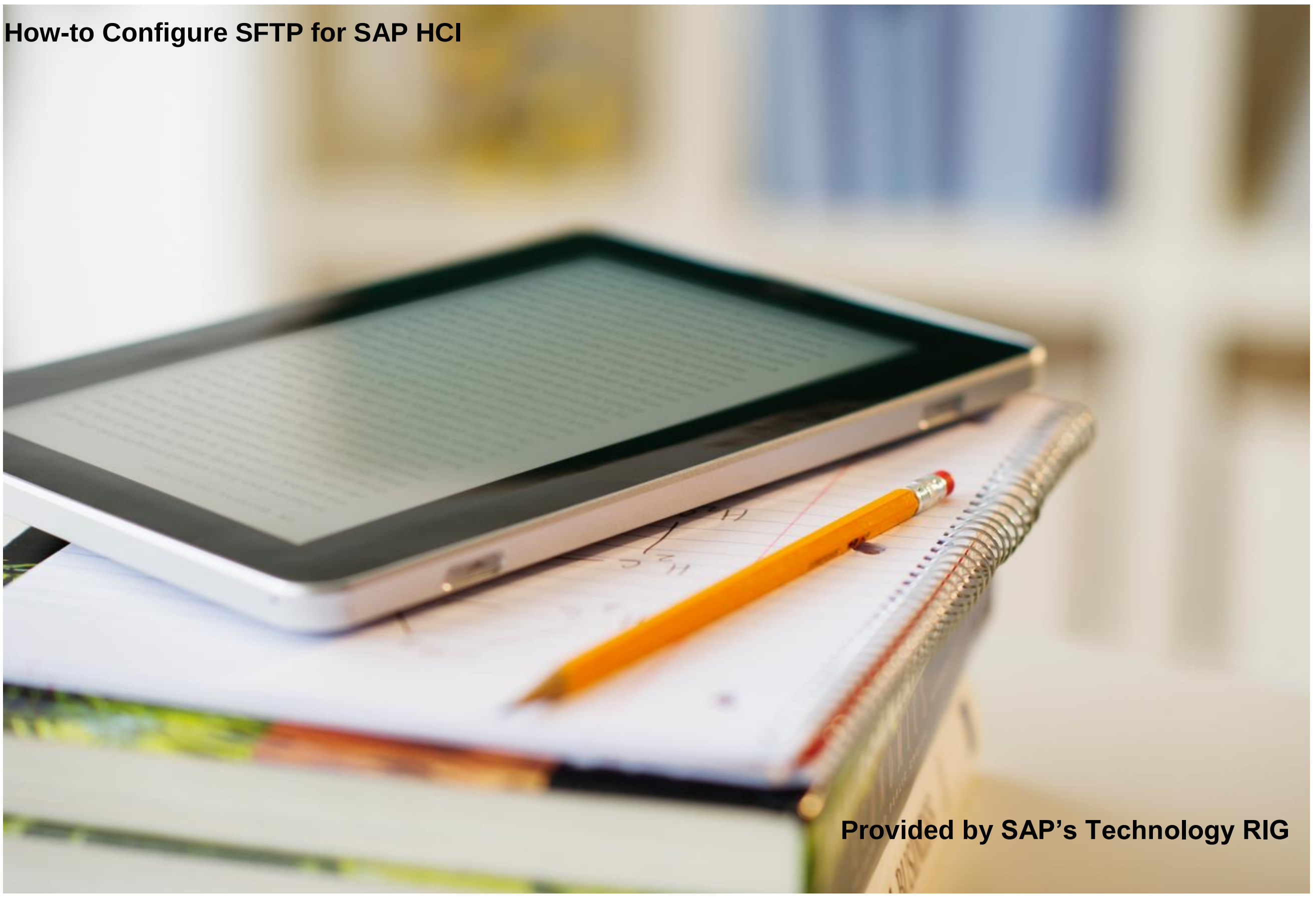


How-to Configure SFTP for SAP HCI
Provided by SAP’s Technology RIG

How-to Configure SFTP for SAP HCI

Applicable Releases:
SAP HCI

Version 1.0 - May 2016

Document History

Document Version	Authored By	Description
1.0	Technology RIG	First release of this guide

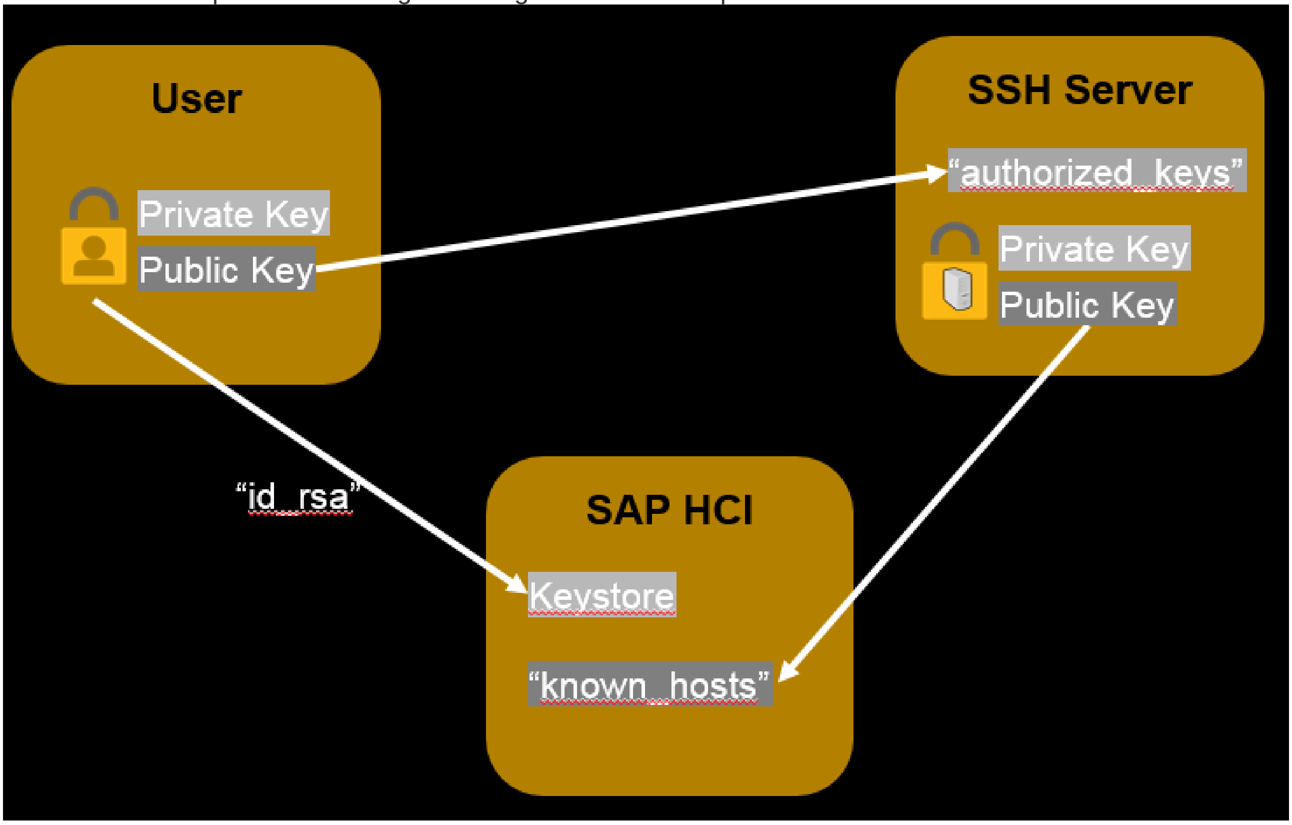
TABLE OF CONTENTS

1. SCENARIO

In this document we will go through the process of connecting your SAP HCI to a SSH server.
We will start with at the beginning with the creation of the SFTP certificate and explain the usage it.
After the setup, we will go step by step though the iFlow creation in the eclipse tool to create a working scenario.

Finally, we will test the connectivity through the eclipse tool and monitor error message during the testing.

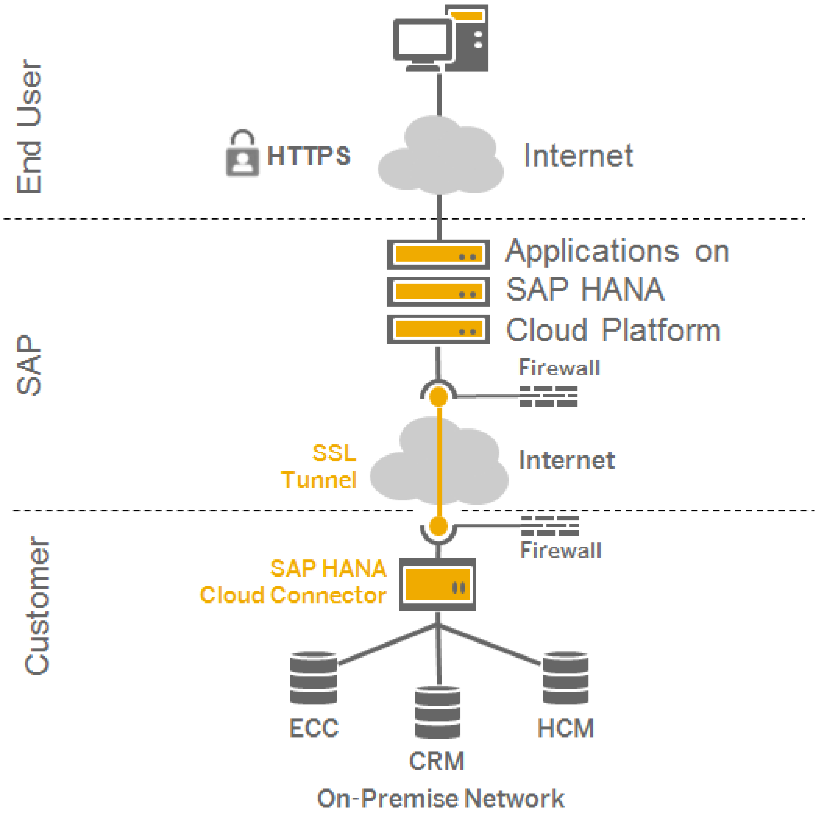
Below is an example of what this guide will guide for the setup.



2. BACKGROUND

The SAP HANA Cloud Platform is the in-memory Platform-as-a-Service offering from SAP, which enables customers and developers to build, extend, and run applications on SAP HANA in the cloud. With flexible subscription models and optional services for apps, database, and infrastructure, it provides instant access to the full power of SAP HANA.

This is the landscape model for the HCP connecting to your backend systems. At this point, we will assumed the SSH server is reachable from the internet so this guide will not cover the installation and configuration of the SCC (SAP HANA Cloud Connector). You can use this guide for the installation of SCC (http://scn.sap.com/docs/DOC-62871).


End User
HTTPS
Internet
SAP
Applications on SAP HANA Cloud Platform
Firewall
SSL Tunnel
Internet
Customer
Firewall
SAP HANA Cloud Connector
ECC
CRM
HCM
On-Premise Network

3. PREREQUISITES FOR THE EXERCISE

The prerequisites for this will vary but below is list what we will be using during this exercise.

- SAP HCI instance – have the ability to modify the keystore on the tenant
- SSH Server – access to an instance of SSH server for testing (SFTP)
- Cygwin – use to create certificate (you could use other tool as well such as PuTTYgen)
    - Package:
        - openSSL
        - openSSH
        - putty – optional if you want to create .ppk file to test with SFTP client
- Eclipse IDE – use to develop iFlow (assumed you have configure the tool to use with SAP HCI)
- KeyStore Explorer – use to manage the java keystore. (http://keystore-explorer.sf.net)

4. STEP-BY-STEP PROCEDURE

This is the overall sequence of steps in the Exercise:

1. Generate Key Pair
2. Create “known_hosts” file
3. Create .ppk for testing with SFTP client
4. Exchange public key with SSH Server
5. Test Using a SFTP Client
6. Deploy the “known_hosts” file to the SAP HCI tenant
7. Update SAP HCI Tenant Keystore with SFTP User Certificate
8. Another Quick Test
9. SFTP Adapter Usage in an iFlow

4.1 Generate Key Pair

The generation of the key pair is important and there are variety of tools that you can use to do this. For this guide, we will be using to the ssh-keygen tool to create the keys. This would allow us to connect to the SFTP server using a client software for testing or to retrieve the data. The screen shot in this guide is for Cygwin.

1. Start the “Cygwin” console

2. Generate a key pair by executing the following command

   ssh-keygen -C <comment> -F <output filename>

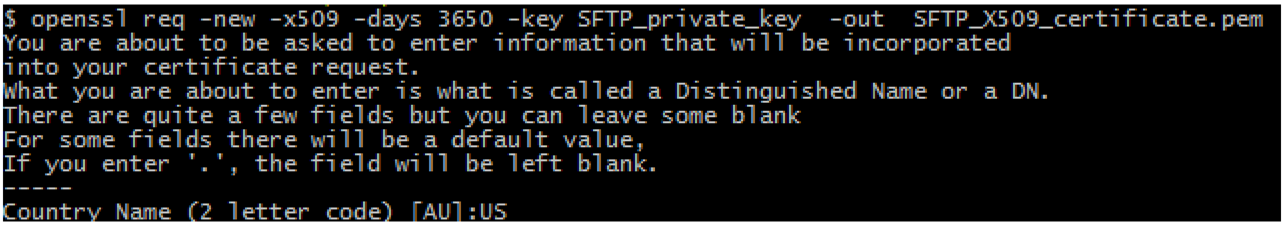
   Example: ssh-keygen -C "SFTP_SAP_HCI" -f SFTP_private_key

   Note: Input some comment about the key itself in the comment parameter

3. Create an X509 certificate by running the following command in the console.

   openssl req -new -x509 -days 3650 -key <key_file> -out <output_file.pem>

   Example: “openssl req -new -x509 -days 3650 -key SFTP_private_key -out SFTP_X509_certificate.pem”



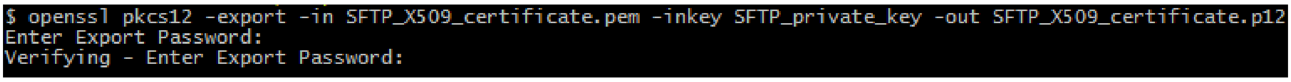
```
$ openssl req -new -x509 -days 3650 -key SFTP_private_key  -out  SFTP_X509_certificate.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
```

Note: follow the on screen instruction to create the X509 certificate.

4. Create a .P12 certificate by running the following command in the console.

   openssl pkcs12 -export -in <x509_certificate_file.pem> -inkey <private_key_file> -out <output_file.p12>

   Example: "openssl pkcs12 -export -in SFTP_X509_certificate.pem -inkey SFTP_private_key -out SFTP_X509_certificate.p12"



```
$ openssl pkcs12 -export -in SFTP_X509_certificate.pem -inkey SFTP_private_key -out SFTP_X509_certificate.p12
Enter Export Password:
Verifying - Enter Export Password:
```

Note: input a password for the file and remember this password for later usage.

5. At this point, you should have 4 files with the following name:
   - "SFTP_private_key" – private key for a user ID (use this to create other)
   - "SFTP_private_key.pub" – public key that will be share with SSH server
   - "SFTP_X509_certificate.pem" – X509 certificate
   - "SFTP_X509_certificate.p12" – this will be import into the keystore for authentication with the SSH server

   Note: It is important to keep either .p12 file or the private key itself since either file may be use later to generate other file format.

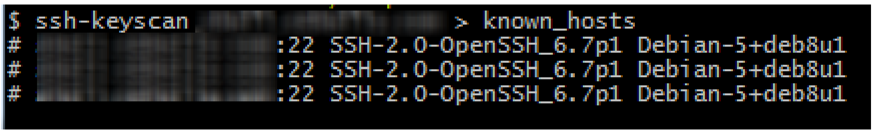
4.2 Create "known_hosts" File

There are other method of getting the public key of the SSH server to create the "known_hosts" file. One method is to ask the admin for the SSH server for the RSA public key of the server. Another method is to use any client that can perform the SSH connection to the host and retrieve the public key.

1. Within the "Cygwin" console, executing the following command.

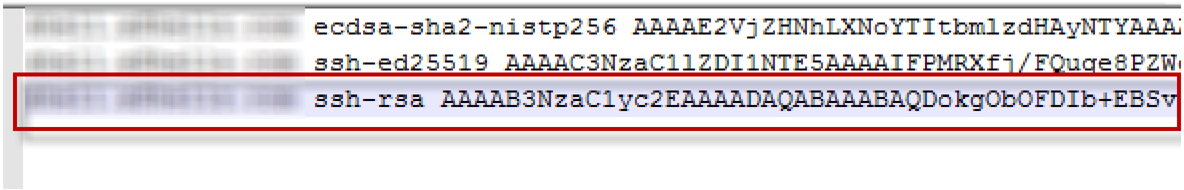
   ssh-keyscan <destination host> > <filename>

   Example: ssh-keyscan mysshserver.sap.com > known_host



```
$ ssh-keyscan [redacted] > known_hosts
# [redacted]:22 SSH-2.0-OpenSSH_6.7p1 Debian-5+deb8u1
# [redacted]:22 SSH-2.0-OpenSSH_6.7p1 Debian-5+deb8u1
# [redacted]:22 SSH-2.0-OpenSSH_6.7p1 Debian-5+deb8u1
```

2. Open the result for editing ("known_hosts") and remove all the all the other line except the line that contain the "ssh-rsa" after the destination hostname. Example:



```
[redacted] ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAA
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFPMRXfj/FQuge8PZW
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDokgObOFDIb+EBSv
```

3. Save the result

4.3 Create .ppk for Testing with SFTP Client

This step is optional if you are planning to use the SFTP client to test the X509 certificate login.

1. Within the “Cygwin” console, executing the following command.
   puttygen <input key file> -O <output key format> -o <output file>
   Example: puttygen SFTP_private_key -O private -o SFTP_private_key.ppk

```
$ puttygen SFTP_private_key -O private -o SFTP_private_key.ppk
```

4.4 Exchange Public Key with SSH Server

Now that we have created and gathered all the necessary file for the setup of the trust between User and SSH server, we will need to exchange the public key to achieve this.

1. If you don’t have access to the SSH server console
   a. Give the user public key (“SFTP_private_key.pub”) to the SSH server administrator and ask him/her to add it to the “authorized_keys” file for the user

2. If you have access to the SSH server console
   a. “ssh” into the SSH server console
   b. Create an “.ssh” directory if it does not exist. **Example:** “mkdir .ssh”
   c. Change to the “.ssh” directory. **Example:** “cd .ssh“
   d. Create a file call “authorized_keys” and copy the content of “SFTP_private_key.pub” into it
      Note: please ensure that you copy it exactly (no line break or add any extra space in the key)
   e. Save the file

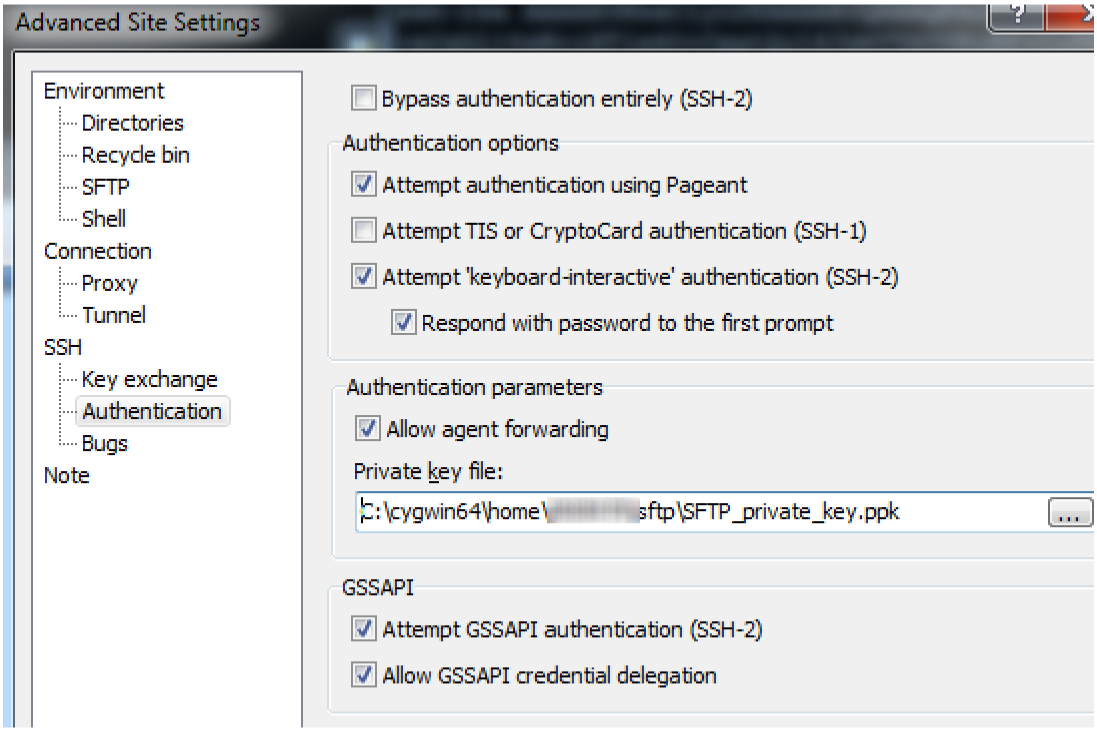
4.5 Test Using a SFTP Client

This step is optional and that you have create the .ppk file for the client to use.

1. Start any SFTP client you have. Example: “WinSCP”

2. Input the basic information about the host, port, & user ID

3. Click on “Advanced…” and select “Authentication” then point to the .ppk file that was created earlier


Advanced Site Settings

Environment
- Directories
- Recycle bin
- SFTP
- Shell

Connection
- Proxy
- Tunnel

SSH
- Key exchange
- Authentication
- Bugs

Note

□ Bypass authentication entirely (SSH-2)

Authentication options

☑ Attempt authentication using Pageant

□ Attempt TIS or CryptoCard authentication (SSH-1)

☑ Attempt 'keyboard-interactive' authentication (SSH-2)

☑ Respond with password to the first prompt

Authentication parameters

☑ Allow agent forwarding

Private key file:

C:\cygwin64\home\[redacted]sftp\SFTP_private_key.ppk ...

GSSAPI

☑ Attempt GSSAPI authentication (SSH-2)

☑ Allow GSSAPI credential delegation

4. Save the setting

5. Click “Login”
   Note: The client should handle the certificate base logon without prompting for any userID/password

6. This will indicate that the public certificate exchange with the SSH Server is correct.

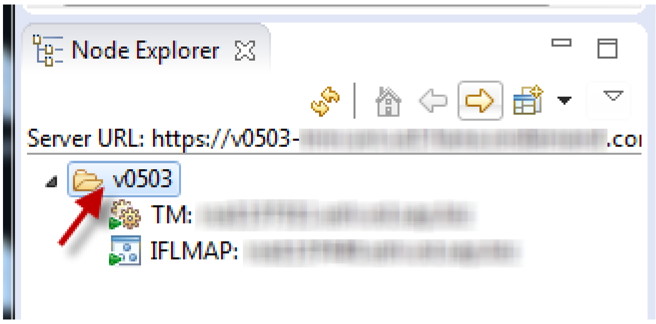
4.6 Deploy the “known_hosts” file to the SAP HCI tenant

For this part of the guide, we will assumed that you have permission/role to deploy artifact to the SAP HCI tenant. If you do not then you can open a support ticket and ask them to deploy it.

Note: if the SAP HCI tenant already have a “known_hosts” file then merge the two files (current file in SAP HCI tenant & new file that was created) together to create a single file before deploy it to the tenant.

1. Start the eclipse studio and connect to the SAP HCI tenant

2. Double click on the tenant ID in the “Node Explorer”



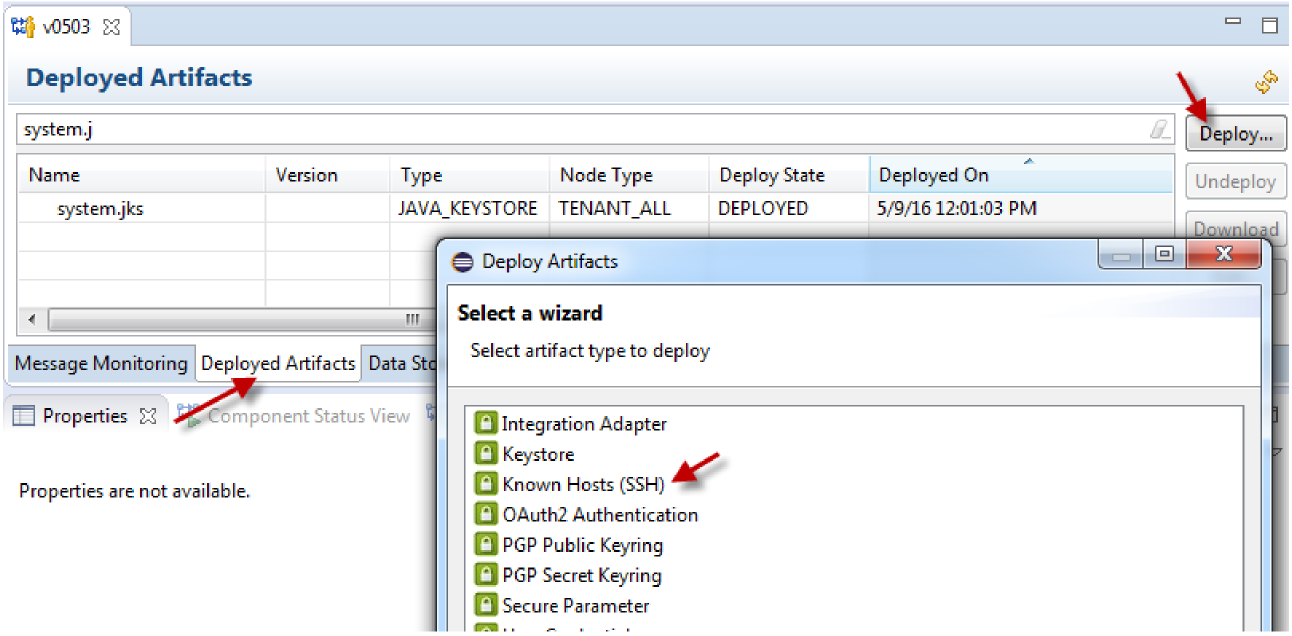
Server URL: https://v0503-[redacted].coı

v0503
- TM: [redacted]
- IFLMAP: [redacted]

3. Click on the “Deployed Artifacts” tab on the new pop-up screen

4. Click “Deploy…” button

5. Select “Known Hosts (SSH)”



Name	Version	Type	Node Type	Deploy State	Deployed On
system.jks		JAVA_KEYSTORE	TENANT_ALL	DEPLOYED	5/9/16 12:01:03 PM

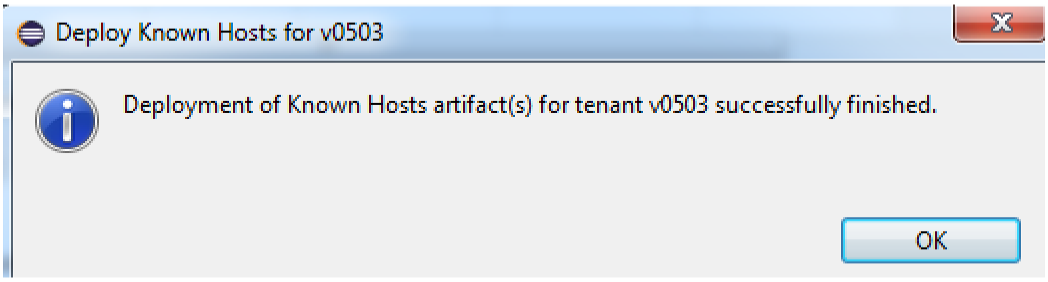
Properties are not available.

Select a wizard

Select artifact type to deploy

6. Browse to the “known_hosts” that we create earlier with the “ssh-keyscan” command (see section “Create “known_hosts” File”).

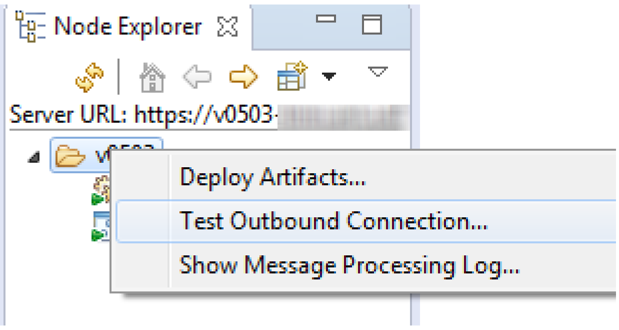
7. Click “Finish” when done



Deploy Known Hosts for v0503

Deployment of Known Hosts artifact(s) for tenant v0503 successfully finished.

8. At this point, we can test the “SSH” connection to the destination host within the eclipse tool
    a. Right click on the SAP HCI tenant on the “Node Explorer” and select “Test Outboud Connection…”

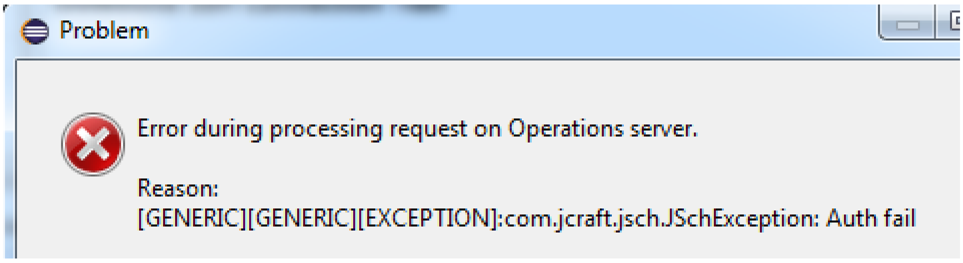

Node Explorer
Server URL: https://v0503-
Deploy Artifacts...
Test Outbound Connection...
Show Message Processing Log...

b. Select “SSH Connection” on the pop-up screen

c. Input the SSH server destination hostname, port, and user ID

d. Click “Run” when finished

e. You should get an error message



Error during processing request on Operations server.

Reason:
[GENERIC][GENERIC][EXCEPTION]:com.jcraft.jsch.JSchException: Auth fail

Note: This failed because SAP HCI tenant does not use the certificate (use incorrect) to authenticate against the SSH server.

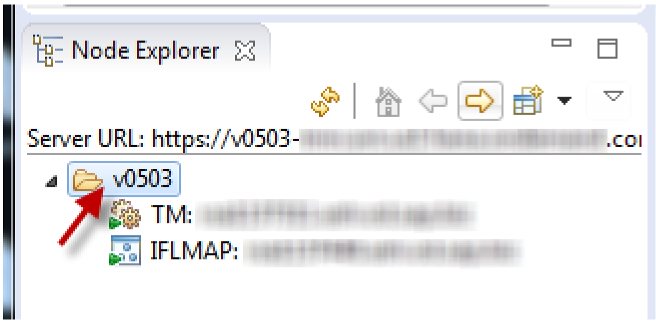
f. This just confirmed that the “known_hosts” file is valid with SAP HCI tenant

4.7 Update SAP HCI Tenant Keystore with SFTP User Certificate

For this part of the guide, we will assumed that you have permission/role to deploy artifact to the SAP HCI tenant. If you do not then you open support ticket and ask them to deploy it.
In addition, you will needs the password for the keystore file that is on the SAP HCI tenant.

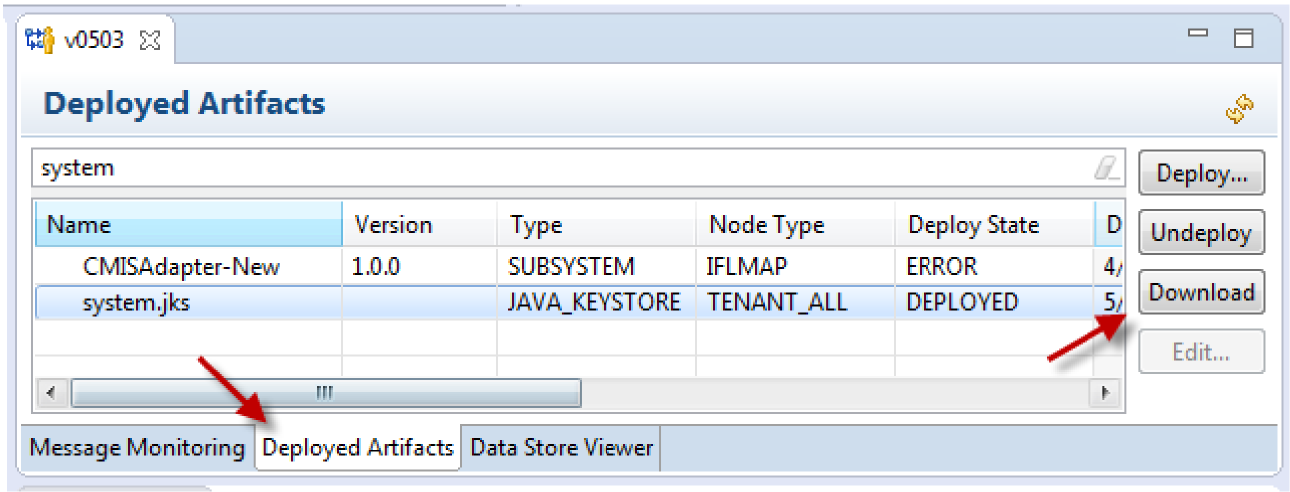
1. Start the eclipse studio and connect to the SAP HCI tenant

2. Double click on the tenant ID in the “Node Explorer”



3. Click on the “Deployed Artifacts” tab on the new pop-up screen

4. Download the “system.jks” file

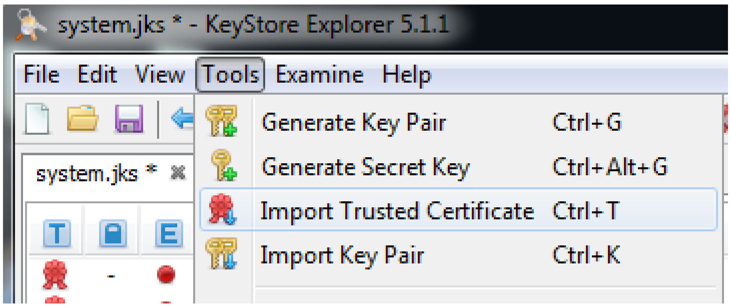


system

Name	Version	Type	Node Type	Deploy State	D
CMISAdapter-New	1.0.0	SUBSYSTEM	IFLMAP	ERROR	4/
system.jks		JAVA_KEYSTORE	TENANT_ALL	DEPLOYED	5/

5. Open the “system.jks” file with “KeyStore Explorer” and input the password

6. Click “Tools” and select “Import Trusted Certficate…”

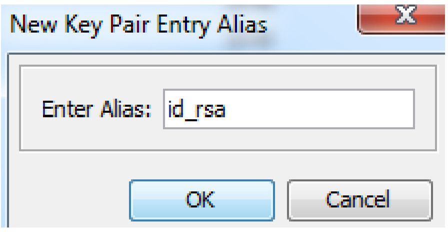


system.jks * - KeyStore Explorer 5.1.1
File
Edit
View
Tools
Examine
Help
system.jks *
T
E
Generate Key Pair Ctrl+G
Generate Secret Key Ctrl+Alt+G
Import Trusted Certificate Ctrl+T
Import Key Pair Ctrl+K

7. Select “PKCS #12” and point to the .p12 file that was created earlier

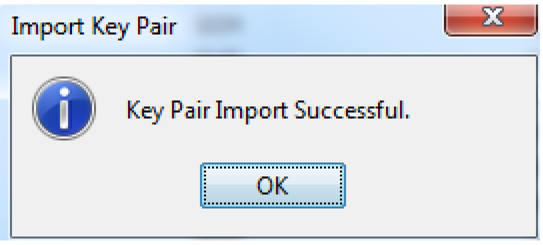
8. Input the password that was set during the creation of the .p12 file then click “Import”

9. On the alias screen, give it the following name “id_rsa”



Enter Alias: id_rsa

10. On the new password screen, please enter the same password that was use by the keystore.

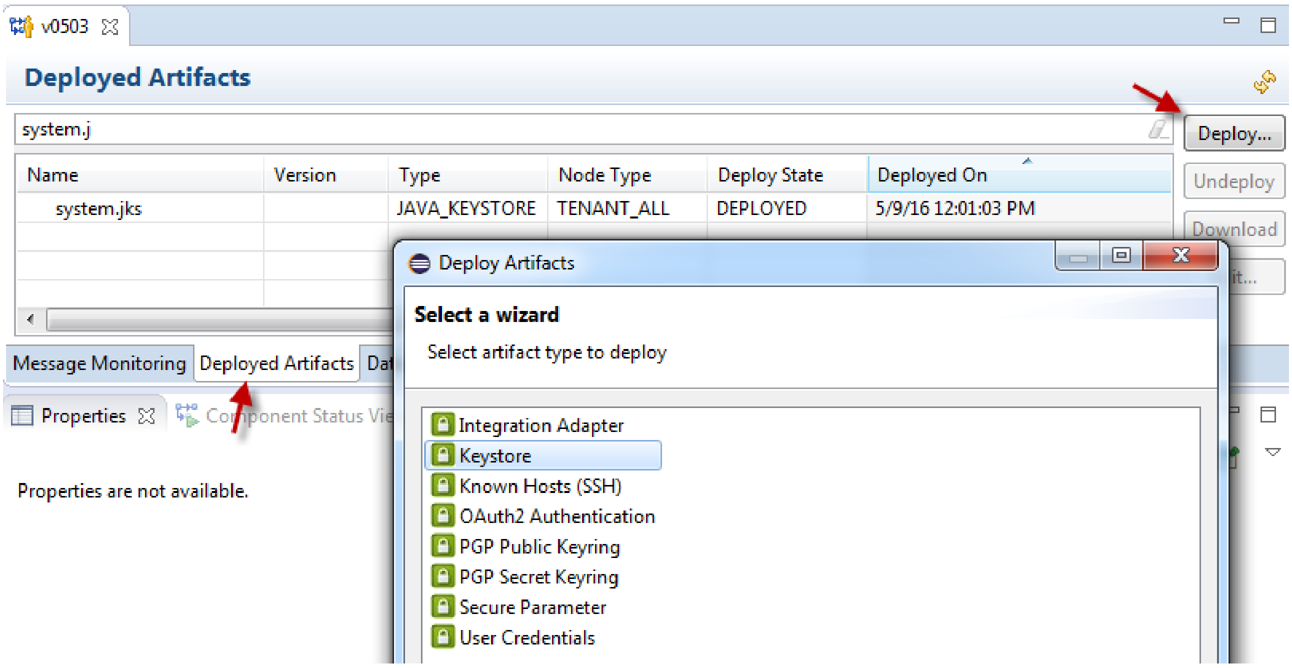


Key Pair Import Successful.

Note: You cannot set another password for this key pair here since SAP HCI will verify the password and reject the deployment.

11. Save the keystore

12. Go back into the eclipse tool and click “Deploy…” in the “Deployed Artifacts” tab



system.j

Name	Version	Type	Node Type	Deploy State	Deployed On
system.jks		JAVA_KEYSTORE	TENANT_ALL	DEPLOYED	5/9/16 12:01:03 PM

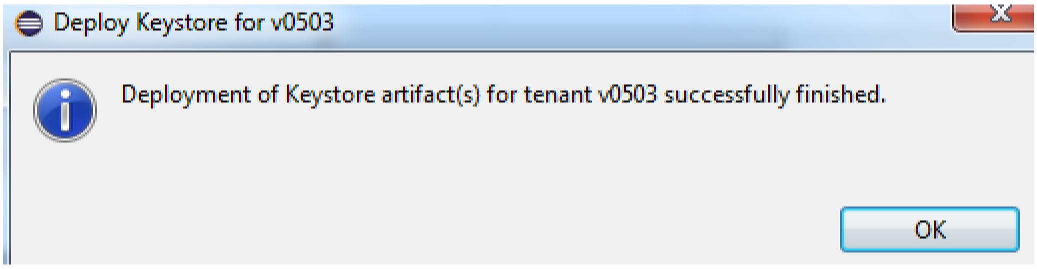
Properties are not available.

Select a wizard

Select artifact type to deploy

- Integration Adapter
- Keystore
- Known Hosts (SSH)
- OAuth2 Authentication
- PGP Public Keyring
- PGP Secret Keyring
- Secure Parameter
- User Credentials

13. Follow the on screen instruction by selecting the updated keystore & input the password.

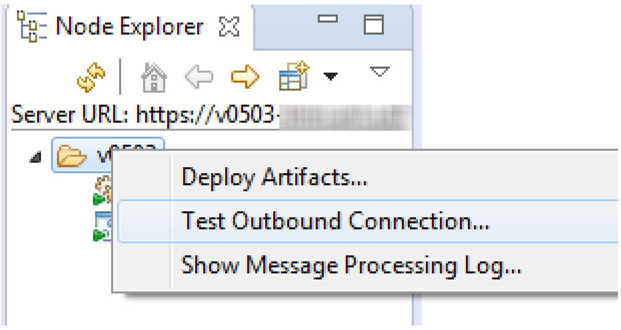


Deployment of Keystore artifact(s) for tenant v0503 successfully finished.

4.8 Another Quick Test

At this point, we have gotten everything setup and ready to go but we can perform another quick test before the actual usage in the iFlow.

1. Right click on the SAP HCI tenant on the “Node Explorer” and select “Test Outboud Connection…”

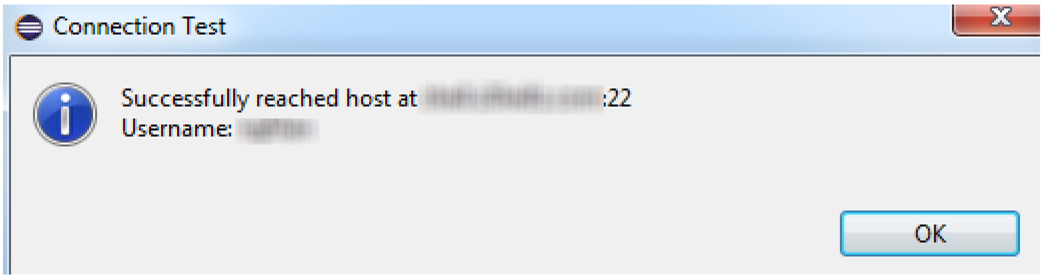


Server URL: https://v0503[redacted]

2. Select “SSH Connection” on the pop-up screen

3. Input the SSH server destination hostname, port, and user ID

4. Click “Run” when finished

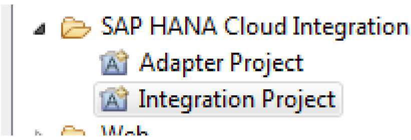


Successfully reached host at [redacted]:22
Username: [redacted]

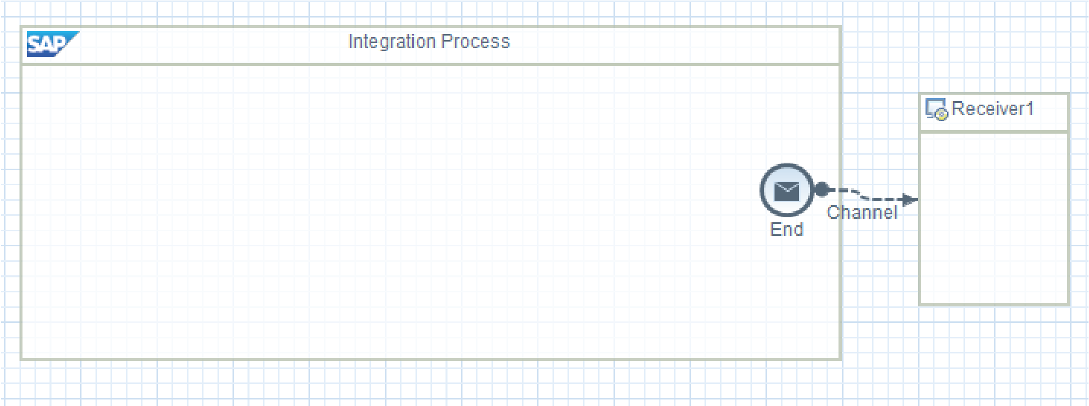
4.9 SFTP Adapter Usage in an iFlow

1. Start Eclipse studio

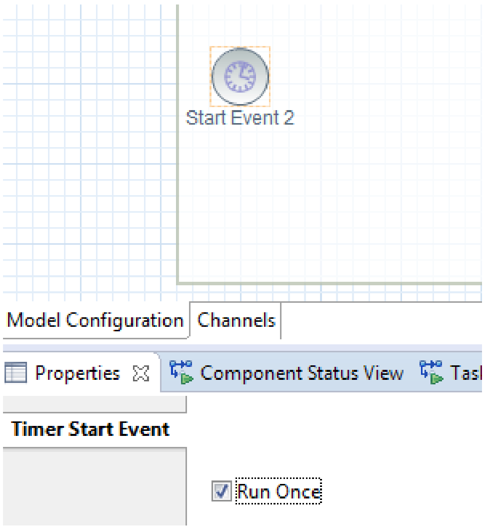
2. Create a new “Integration Project” and give a project name (default everything else)



3. Update the canvas by deleting the unwanted steps (see image below)

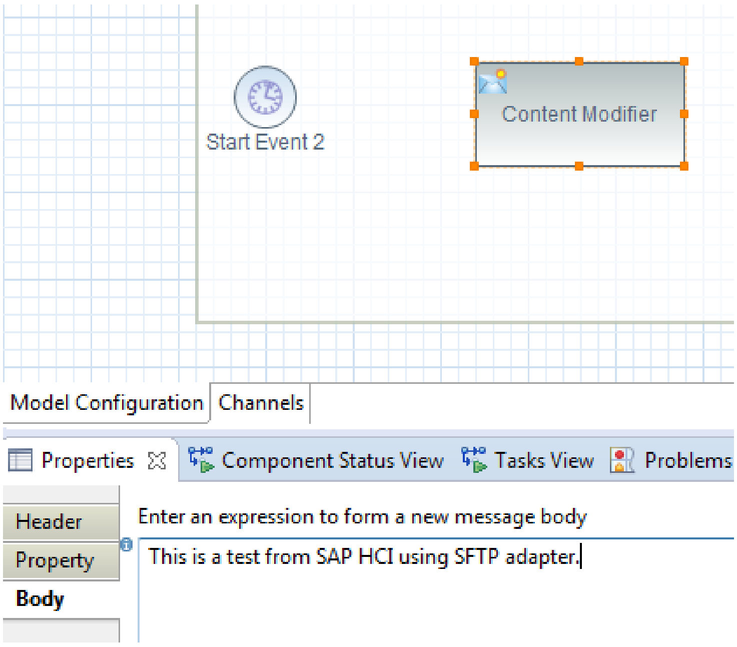


4. Add the timer event (Events->Timer Start) to the canvas and set the property to “Run Once”



☑ Run Once

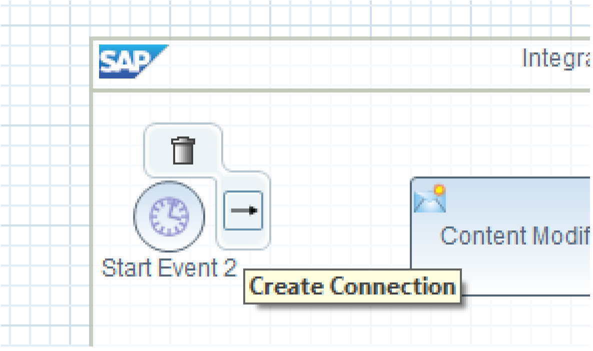
5. Add the “Content Modifier” to the canvas, add some message to the body property.

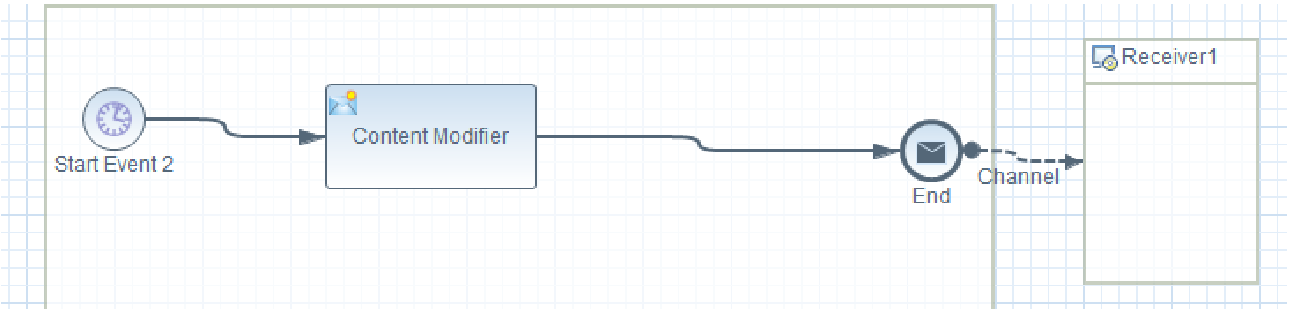


Enter an expression to form a new message body

This is a test from SAP HCI using SFTP adapter.

6. Connect each steps end-to-end to complete the flow.



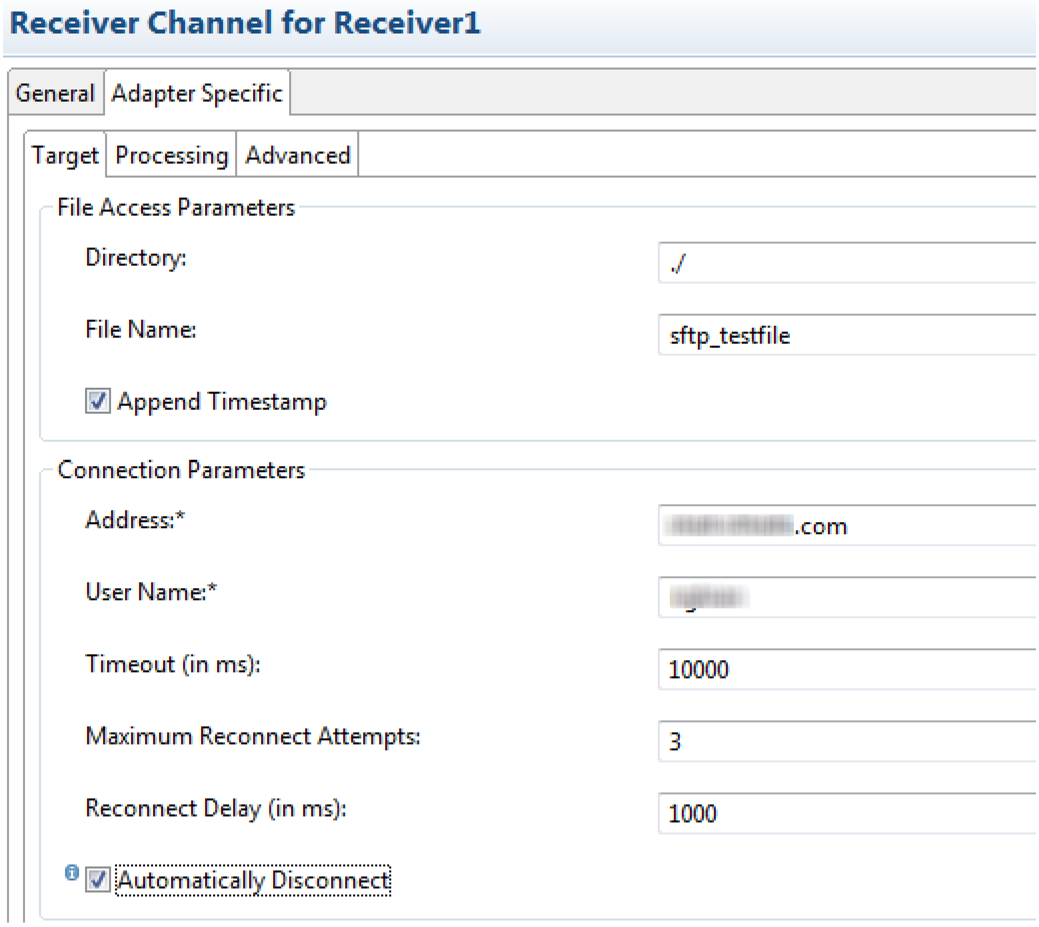


7. Double click on the “Channel” for the “Receiver1”

8. Input some value for the “Name:”

9. Select “SFTP” for the “Adapter Type:”

10. Select “Adapter Specific” tab, you can configure various setting. For this test, we will just input the basic: hostname, directory, filename, and username



Receiver Channel for Receiver1

File Access Parameters

Directory: ./

File Name: sftp_testfile

☑ Append Timestamp

Connection Parameters

Address:* [redacted].com

User Name:* [redacted]

Timeout (in ms): 10000

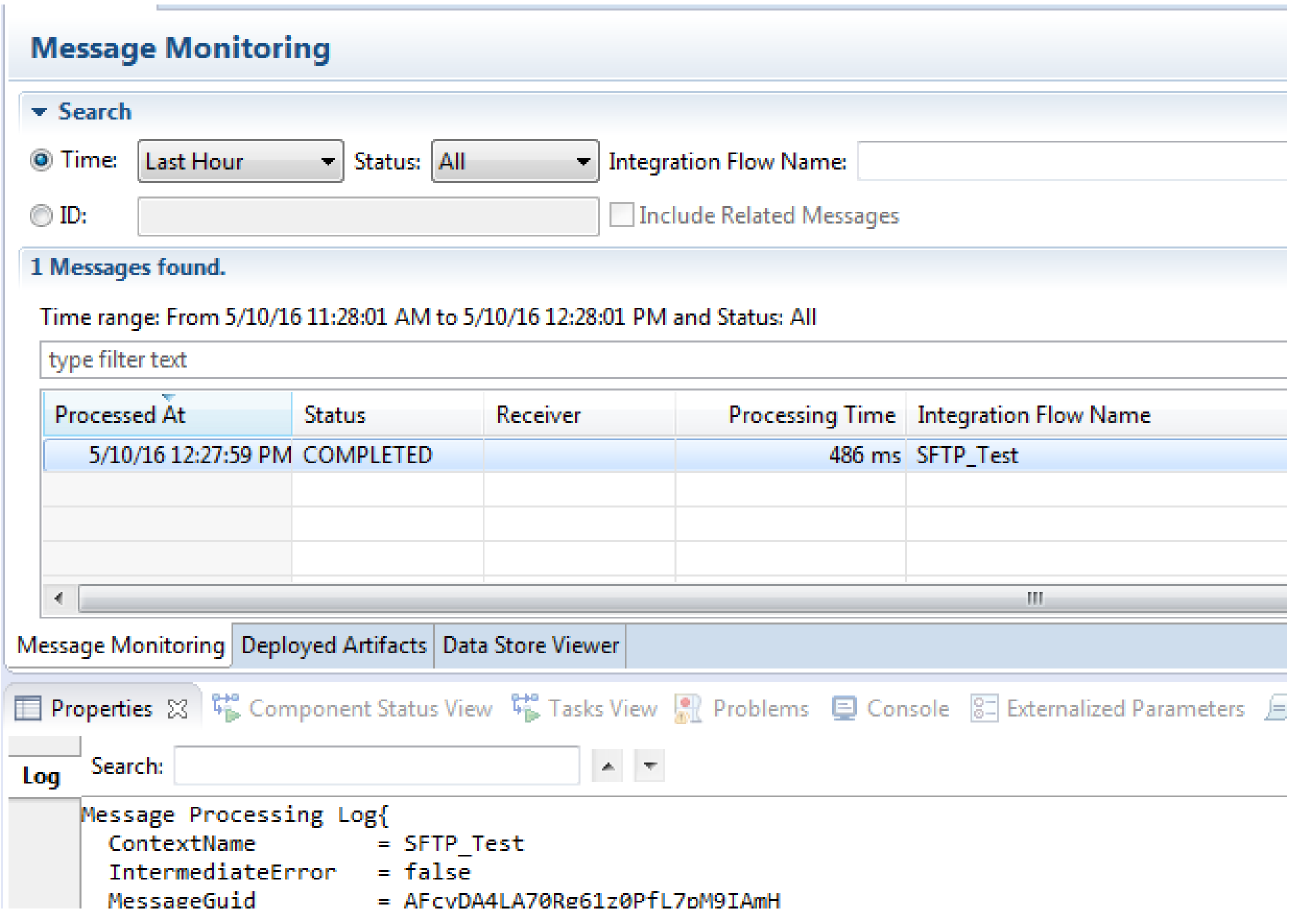
Maximum Reconnect Attempts: 3

Reconnect Delay (in ms): 1000

☑ Automatically Disconnect

11. Save the project & deploy it to the SAP HCI tenant.

12. If successful, you can see result in the monitor tab



● Time: Last Hour ○ Status: All Integration Flow Name:

○ ID: □ Include Related Messages

1 Messages found.

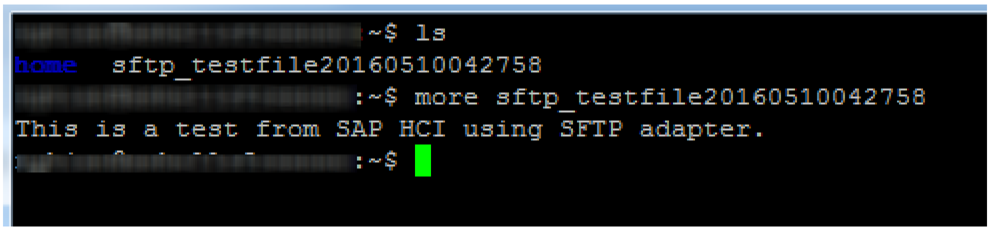
Time range: From 5/10/16 11:28:01 AM to 5/10/16 12:28:01 PM and Status: All

type filter text

Processed At	Status	Receiver	Processing Time	Integration Flow Name
5/10/16 12:27:59 PM	COMPLETED		486 ms	SFTP_Test

```
Message Processing Log{
  ContextName          = SFTP_Test
  IntermediateError    = false
  MessageGuid          = AFcvDA4LA70Rg61z0PfL7pM9IAmH
```

13. On the SSH server itself



```
[redacted]~$ ls
home   sftp_testfile20160510042758
[redacted]:~$ more sftp_testfile20160510042758
This is a test from SAP HCI using SFTP adapter.
[redacted]:~$
```

5. APPENDIX

5.1 Possible Error Message

- Caused by: com.jcraft.jsch.JSchException: reject HostKey: ...
  - **Answer:** SSH server does not match the client key (SAP HCI). Check to ensure the “id_rsa” alias is using the correct key

- Caused by: com.jcraft.jsch.JSchException: Auth cancel
  - **Answer:** “known_hosts” key does not match the SSH server. Use “ssh-keyscan” to get the correct key for the “ssh-rsa” key type
  - **Answer:** invalid or missing user cert in keystore
  - **Answer:** user name in the “SFTP” adapter is not correct

- Caused by: com.jcraft.jsch.JSchException: fromBase64: invalid base64 data
  - **Answer:** “known_hosts” is invalid

- Caused by: com.jcraft.jsch.JSchException: HostKey has been changed: ...
  - **Answer:** “known_hosts” key does not match the SSH server.

- If project does not run
  - **Answer:** check to ensure “known_hosts” file exist

- Caused by: com.sap.cloud.crypto.keystore.api.KeyStoreNotFoundException: Keystore with name: 'known.hosts' is not found neither in the cloud (domain db) nor in the local (file) storage
  - **Answer:** check to ensure “known_hosts” file exist

www.sap.com

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.